Claims

WHAT IS CLAIMED IS:

1	1.	A method for polic	y and attribute based access to a resource,	comprising:

- 2 interacting with a principal for authenticating the principal based on acquired
- 3 identity information;
- 4 assembling an identity configuration for the principal;
- 5 generating a service contract for the principal, a service, and a resource,
- 6 wherein the principal uses the service to access the resource, and wherein the
- 7 service contract includes a selective number of resource access policies and
- 8 attributes which are included in the identity configuration; and
- 9 transmitting an access statement to the principal for use when the principal
- 10 interacts with the service.
- 1 2. The method of claim 1 further comprising generating alias identity
- 2 information for the identity information and including the alias identity information
- 3 with at least a portion of the access statement.
- 1 3. The method of claim 2 further comprising:
- 2 receiving the alias identity information from the service;
- mapping the alias identity information back to the identity information;
- 4 authenticating the identity information; and
- 5 permitting the service to the resource based on the service contract.
- 1 4. The method of claim 1 wherein the transmitting of the access statement
- 2 further includes representing the access statement as an assertion that is directly
- 3 used to acquire the identity information of the principal.
- 1 5. The method of claim 1 wherein the transmitting of the access statement
- 2 further includes representing the identity information of the principal as an artifact

Attorney Docket No.: 1565.060US1 25

- 3 that can be indirectly used to acquire the identity information.
- 1 6. The method of claim 1 further comprising removing the service contract
- when an active session with the principal expires.
- 1 7. The method of claim 1 wherein the interacting further includes establishing a
- 2 secure communication with the principal.
- 1 8. A method for policy and attribute based access to a resource, comprising:
- 2 receiving a session request for access to a resource, wherein the session
- 3 request is sent from a service and includes alias identity information for a principal;
- 4 mapping the alias identity information to identity information of the
- 5 principal;
- 6 authenticating the identity information;
- acquiring a service contract for the principal, the service, and the resource,
- 8 wherein the service contract includes selective resource access policies and
- 9 attributes which are permissibly used by the service on behalf of the principal; and
- establishing a session with the service, wherein the session is controlled by
- 11 the service contract.
 - 1 9. The method of claim 8 further comprising accessing an identity
 - 2 configuration for the principal in order to acquire the selective resource access
 - 3 policies and attributes included within the service contract.
 - 1 10. The method of claim 8 further comprising denying access attempts made by
 - 2 the service during the session when the access attempts are not included within the
 - 3 service contract.
 - 1 11. The method of claim 8 further comprising terminating the session when an
 - 2 event is detected that indicates the service contract is compromised or has expired.

- 1 12. The method of claim 8 further comprising establishing the service contract
- 2 with the principal prior to receiving the session request.
- 1 13. The method of claim 12 further comprising reusing the service contract to
- 2 establish one or more additional sessions with the service, wherein the one or more
- 3 additional sessions are associated with one or more additional session requests made
- 4 by the service.
- 1 14. The method of claim 12 wherein the establishing further includes
- 2 establishing the service contract with the principal in response to a redirection
- 3 operation performed by a proxy that intercepts a browser request issued from the
- 4 principal to the service for purposes of accessing the resource.
- 1 15. A policy and attribute based resource access system, comprising:
- 2 an identity authenticator;
- an identity configuration aggregator; and
- 4 a resource session administrator;
- wherein the identity authenticator authenticates a principal for access to a
- 6 resource based and generates a service contract, and wherein the identity
- 7 configuration aggregator generates an identity configuration for the principal and
- 8 the resource, the service contract defines selective resource access policies and
- 9 attributes from the identity configuration, and wherein the resource session
- administrator establishes a session with a service and ensures that access attempts
- 11 made by the service during the session conform to the service contract.
 - 1 16. The policy and attribute based resource access system of claim 15 wherein
 - 2 the system is implemented as a proxy server.
 - 1 17. The policy and attribute based resource access system of claim 15 wherein
 - 2 the service contract is generated in response to an intercepted resource-access
 - 3 request made by the principal to the service.

- 1 18. The policy and attribute based resource access system of claim 17, wherein
- 2 the resource-access request is redirected by a Hyper Text Transfer Protocol (HTTP)
- 3 Proxy serving as an intermediary between the principal and the service.
- 1 19. The policy and attribute based resource access system of claim 15, wherein
- 2 the service contract is generated in response to a redirected resource-access request
- 3 made by the principal to the service, and wherein the service redirects the resource-
- 4 access request to the system.
- 1 20. The policy and attribute based resource access system of claim 15, wherein
- 2 the service contract expires when an active session with the principal expires.
- 1 21. A policy and attribute based resource session manager, residing in a
- 2 computer-accessible medium, comprising instructions for establishing a session
- 3 with a resource, the instructions when executed performing the method of:
- 4 receiving alias identity information from a service, wherein the alias identity
- 5 information is associated with a principal;
- 6 requesting a mapping of the alias identity information to principal identity
- 7 information;
- 8 requesting authenticating of the identity information;
- 9 requesting a service contract for the principal, the service and a resource,
- wherein the service contract includes selective resource access policies and
- 11 attributes derived from an identity configuration; and
- establishing a session with the service and the resource, wherein the session
- is controlled by the service contract.
- 1 22. The policy and attribute based resource session manager of claim 21 having
- 2 instructions further comprising, permitting the service to indirectly access an
- 3 identity store which represents the resource, and wherein the identity store includes
- 4 secure information related to the principal.

- 1 23. The policy and attribute based resource session manager of claim 21 having
- 2 instructions further comprising terminating the session when the service contract
- 3 expires or is compromised.
- 1 24. The policy and attribute based resource session manager of claim 21,
- 2 wherein the requesting of the mapping further includes interacting with an alias
- 3 translator.

1 🎍

- 1 25. The policy and attribute based resource session manager of claim 21,
- 2 wherein the requesting of authentication further includes interacting with an
- 3 identification authenticator.
- 1 26. The policy and attribute based resource session manager of claim 21 having
- 2 instructions further comprising managing the session by acting as an intermediary
- 3 between the service and a legacy Lightweight Directory Access Protocol (LDAP)
- 4 application which has access privileges to the resource.
- 1 27. The policy and attribute based resource session manager of claim 26,
- 2 wherein the receiving further includes intercepting a session request that is issued
- 3 from the service for the legacy LDAP application, wherein the session request
- 4 includes the alias identity information.
- 1 28. The policy and attribute based resource session manager of claim 27 having
- 2 instructions further comprising managing the session with respect to the service as if
- 3 the policy based resource session manager were the legacy LDAP application.
- 1 29. The policy and attribute based resource session manager of claim 21 wherein
- 2 the instructions for establishing the session further includes defining the selective
- 3 resource access policies as at least one of a read operation and a write operation and
- 4 defining the attributes as selective confidential data related to the principal, wherein

Attorney Docket No.: 1565.060US1 29

- 5 the policies define operations that are permissible on the attributes, and wherein
- 6 values for the attributes reside in the resource.